

Listing and Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) A communications system, comprising:
a gateway connected to a wired network; and
a plurality of access points associated with, and controlled by, the gateway,
wherein each access point is configured (i) (a) to wirelessly communicate with and receive association requests from wireless clients for connection to the wired network through the access point (ii) (b) to send session information requests to the gateway in response to received association requests and (iii) (c) to process session information setting commands received from the gateway,
wherein the gateway is configured (i) to maintain session information that currently exists for each wireless client connected to the wired network through an access point associated with the gateway, the session information including a session key associated with each wireless client and an associated access point, and (ii) to respond to a session information request from a given access point by providing that access point with currently existing session information, if any, maintained by the gateway for the wireless client requesting association with that access point; and
wherein each access point is configured to maintain the session key per associated wireless client.
2. (Cancelled)
3. (Previously presented) The system of claim 1 wherein each access point is configured to remove session information after a wireless client becomes disassociated with that access point by either responding to a command sent to the access point from the gateway to remove the session information or automatically removing idle wireless client session information entries after a predetermined period of inactivity.

4. (Original) The system of claim 1 having means to ensure that a connection between the gateway and an access point is trusted.
5. (Original) The system of claim 4 wherein the means comprises physical security or encryption.
6. (Previously presented) A method of enabling roaming of wireless clients among wireless access points in a network comprising the steps of (a) providing a gateway in the network in control of the wireless access points, sending session data requests from access points to the gateway, the session data including a session key associated with each wireless client and an associated access point, (b) looking up session data stored in the gateway, reporting session data failure if session data is not found, and (c) sending a session data response from the gateway to the access point if session data is found or is generated by the gateway;
wherein an association request from a wireless client is received by an access point and, after receiving a session data failure response from the gateway, the access point generates session data, reports the generated session data to the gateway and sends an association response to the wireless client.
7. (Original) The method of claim 6 wherein an association request from a wireless station is received by an access point and, after receiving a session data response from the gateway, the access point loads session data and sends the session data to the wireless client.
8. (Cancelled)
9. (Previously presented) The method of claim 6 comprising removing session information from the previously associated access point after a wireless client becomes associated with a new access point comprising the gateway sending a command to the previously associated access point to remove the session information or automatically removing idle wireless client entries after a predetermined period of inactivity.

10. (Original) The method of claim 6 wherein the gateway authenticates an access point to ensure that a connection between the gateway and the access point is trusted.
11. (Original) The method of claim 10 wherein the authentication is encrypted.
12. (Cancelled)
13. (Previously presented) A non-transitory computer readable medium encoded with instructions that are executable by a processor in a wireless access point in a network for the wireless access point device to perform the steps of:
- receiving an association request from a wireless client;
 - communicating with a gateway connected to the network to obtain currently existing session information maintained by the gateway, if any, which is associated with the wireless client requesting association to the wireless access point, the session information comprising a session key associated with the wireless client and an associated wireless access point;
 - receiving a session data response from the gateway, which includes currently existing session information for the wireless client requesting association to the wireless access point;
 - and
 - loading the session information into the wireless access point and sending the session information to the wireless client in an association response transmitted to the wireless client.
14. (Previously presented) The computer readable medium of claim 13, further encoded with instructions executable by the processor for the wireless access point to perform steps of:
- receiving a session data failure response from the gateway indicating that no session information currently exists for the wireless client, and
 - in response to said received data failure response, generating session data, reporting the generated session data to the gateway and sending an association response to the wireless client.

15. (Previously presented) The computer readable medium of claim 13, further encoded with instructions executable by the processor for the wireless access point to perform a step of removing session information for a wireless client previously associated with the wireless access point after the wireless client becomes associated with a new wireless access point.

16. (Previously presented) The computer readable medium of claim 13, further encoded with instructions that are executable by the processor of the wireless access point device to perform an authentication process to ensure that a connection between the gateway and the wireless access point is trusted.

17. (Previously presented) The computer readable medium of claim 16 wherein the authentication comprises encrypted communications with the gateway.

18. (Previously presented) The computer readable medium of claim 15, wherein removing session information for the wireless client is performed by the wireless access point in response to a command sent by the gateway to remove that session information.

19. (Previously presented) The computer readable medium of claim 15, wherein removing session information for a wireless client is performed automatically by the wireless access point removing idle wireless client session information entries for the wireless client after a predetermined period of inactivity of the wireless client.

20. (New) The computer readable medium of claim 13, wherein the session data response from the gateway includes an indication of session information failure if no session information for the wireless client is found.

21. (New) The system of claim 1, wherein the gateway is further configured to report session information failure if no session information for the wireless client is found.

22. (New) The system of claim 21 wherein each access point is configured to remove session information after a wireless client becomes disassociated with that access point by either responding to a command sent to the access point from the gateway to remove the session information or automatically removing idle wireless client session information entries after a predetermined period of inactivity.

23. (New) The system of claim 21 having means to ensure that a connection between the gateway and an access point is trusted.

24. (New) The system of claim 23 wherein the means comprises physical security or encryption.